CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (currently amended) A method of ~~generating a~~ linear transformation ~~matrix A by a device for use~~ in a symmetric-key cipher ~~, the method including~~ comprising:

inputting block data into a processing apparatus;

creating a linear transformation matrix A with the processing apparatus by:

generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a ~~standard~~ form $G = (I_k \parallel B)$, with $B \in Z_2^{k \times (n-k)}$, where k < n < 2k, and d is the minimum distance of the binary error-correcting code;

shortening said error-correcting code; and

extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving the linear transformation matrix A from matrix C; and

transforming the input block data into diffused output block data with the processing apparatus by using the linear transformation matrix A.

2. (currently amended) A method as claimed in claim 1, wherein extending matrix B with 2k-n columns ~~includes~~ comprises:

in an iterative manner:

randomly generating 2k-n columns, each with k binary elements;

forming a test matrix consisting of the n-k columns of B and the 2k-n generated columns; and

checking whether the test matrix is non-singular, until a non-singular test matrix has been found; and

using the found test matrix as matrix C.

3. (currently amended) A method as claimed in claim 1, wherein the operation ~~step~~ of deriving matrix A from matrix C ~~includes~~ comprises:

determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix (I_k || P_1 C P_2), have a predetermined multi-bit weight; and

using P_1 C P_2 as matrix A.

4. (currently amended) A method as claimed in claim 3, wherein the input block data is m-bit sub-block data, and the processing apparatus executes ~~cipher includes~~ a round function with an S-box layer with S-boxes operating on the m-bit sub-block~~s~~ data, and the minimum predetermined multi-bit weight over all non-zero codewords equals a predetermined m-bit weight.

5. (currently amended) A method as claimed in claim 3, wherein determining the two permutation matrices P_1 and P_2 ~~includes~~ comprises iteratively generating the matrices in a random manner.

6. (currently amended) A method as claimed in claim 1, wherein the ~~cipher includes a round function operating on~~ input block data is 32-bit block data ~~blocks~~ and wherein the ~~step~~ operation of generating a [n,k,d] error-correcting code ~~includes~~ comprises:

generating a binary extended Bose-Chaudhuri-Hocquenghem (XBCH) [64,36,12] code; and

shortening ~~this~~ the XBCH [64,36,12] code to a [60,32,12] ~~shortened~~ XBCH code by deleting four rows.

7. (currently amended) A computer program product stored on a computer readable medium, wherein the program product is operative to cause the ~~a~~ processor to perform the method of claim 1.

8. (currently amended) A system for cryptographically converting an input data block into an output data block[[;]], the input data blocks comprising n data bits[[;]], the system ~~including~~ comprising:

an input for receiving the input data block;

a storage for storing a linear transformation matrix A ~~, generated according to the method of claim 1,~~ created by:

generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where $k < n < 2k$, and d is the minimum distance of the binary error-correcting code;

shortening said error-correcting code; and

extending matrix B with 2k-n columns such that a resulting matrix C is non-singular, and deriving the linear transformation matrix A from matrix C;

a cryptographic processor performing a linear transformation on the input data block or a derivative of the input data block using the linear transformation matrix A; and

an output for outputting the processed input data block.

9-10. (cancelled)

11. (new) A system as claimed in claim 8, wherein extending matrix B with 2k-n columns comprises:

in an iterative manner:

randomly generating 2k-n columns, each with k binary elements;

forming a test matrix consisting of the n-k columns of B and the 2k-n generated columns; and

checking whether the test matrix is non-singular, until a non-singular test matrix has been found; and

using the found test matrix as matrix C.

12. (new) A system as claimed in claim 8, wherein the operation of deriving matrix A from matrix C comprises:

determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix (I_k || P_1 C P_2), have a predetermined multi-bit weight; and

using P_1 C P_2 as the matrix A.

13. (new) A system as claimed in claim 12, wherein the input block data is m-bit sub-block data, and the processing apparatus executes a round function with an S-box layer with S-boxes operating on the m-bit sub-block data, and the minimum predetermined multi-bit weight over all non-zero codewords equals a predetermined m-bit weight.

14. (new) A system as claimed in claim 12, wherein determining the two permutation matrices P_1 and P_2 comprises iteratively generating the matrices in a random manner.

15. (new) A system as claimed in claim 8, wherein the input data block is a 32-bit data block and wherein the operation of generating a [n,k,d] error-correcting code comprises:

generating a binary extended Bose-Chaudhuri-Hocquenghem (XBCH) [64,36,12] code; and

shortening the XBCH [64, 36, 12] code to a [60, 32, 12] XBCH code by deleting four rows.

16. (new) A method of linear transformation in a symmetric-key cipher comprising:

inputting block data into a processing apparatus;

creating a linear transformation matrix A with the processing apparatus by:

generating a binary [n,k,d] error-correcting code, represented by a generator matrix $G \in Z_2^{k \times n}$ in a form $G = (I_k \| B)$, with $B \in Z_2^{k \times (n-k)}$, where k < n < 2k, and d is the minimum distance of the binary error-correcting code;

extending matrix B with 2k-n columns such that a resulting matrix C is non-singular;

determining two permutation matrices $P_1, P_2 \in Z_2^{k \times k}$ such that all codewords in an [2k,k,d] error-correcting code, represented by the generator matrix $(I_k \| P_1 C P_2)$, have a predetermined multi-bit weight; and

using $P_1 C P_2$ as matrix A; and

transforming the input block data into diffused output block data with the processing apparatus by using the linear transformation matrix A.